Optimal Energy Storage System Placement for Robust Stabilization of Power Systems Against Dynamic Load Altering Attacks

Roberto Germanà, Alessandro Giuseppi*, Antonio Pietrabissa, Alessandro Di Giorgio

***Abstract*— This paper presents a study on the "Dynamic Load Altering Attacks" (D-LAAs), their effects on the dynamics of a transmission network, and provides a robust control protection scheme, based on polytopic uncertainties, invariance theory, Lyapunov arguments and graph theory. The proposed algorithm returns an optimal Energy Storage Systems (ESSs) placement, that minimizes the number of ESSs placed in the network, together with the associated control law that can robustly stabilize against D-LAAs. The paper provides a contextualization of the problem and a modelling approach for power networks subject to D-LAAs, suitable for the designed robust control protection scheme. The paper also proposes a reference scenario for the study of the dynamics of the control actions and their effects in different cases. The approach is evaluated by numerical simulations on large networks.**

***Index Terms*— Dynamic Load Altering Attacks; Energy Storage Systems; Cyber-Physical security;**

NOMENCLATURE

δ, θ	Voltage phase angle at generator/load buses
ω, ϕ	Frequency deviation at generator/load buses
M	Inertia matrix of the generators
n, m	number of generators and load buses
$\mathcal{M}_a, \mathcal{M}_p$	sets of vulnerable and secure buses
$\mathcal{M}_p^*$	optimal placement
$\mathcal{E}$	sets of transmission line
$\mathcal{M}_g$	Set of generation nodes
D, D^L	Damping coefficient matrices for the generators and loads
P^L	Power consumption at load buses
K^P, K^I	Generator controller gain matrices
K^{LG}	Attack gain matrix
α	Decrease rate of the Lyapunov function
u_{max}	Bound on the ESS power norm
Z	Impedance Matrix
$\mathbf{0}_n, \mathbf{1}_n$	Column vectors of zeros and ones of size n
$tr(\cdot)$	Trace of a matrix

I. INTRODUCTION

With the evolution of power systems towards more complex, intelligent, and dynamical systems, the power network has become a critical cyber-physical system (CPS), in which the interaction of the physical domain with the ICT component of the system plays an evermore important role.

This work has been partially supported by Sapienza with the project "PROMETEO - Protezione di reti elettriche di potenza da attacchi ciber-fisici mediante strategie di controllo" project, no. RM11715C7EFAF857.

The authors are with the Department of Computer, Control, and Management Engineering Antonio Ruberti at Sapienza University of Rome, Via Ariosto, 25, 00185 Rome, Italy, and the cyber security research group of CRAT, Via Giovanni Nicotera, 29, 00195 Rome, ITaly

*Corresponding author, email: giuseppi@diag.uniroma1.it.

The digital innovations that are at the basis of the smart grid paradigm, such as demand-side management [1], [2] and vehicle-to-grid services [3], introduced in the power network several vulnerabilities that allow for the design of new and sophisticated attacks [4]–[6], which may deteriorate the power quality or even interrupt the service provision.

Among such cyber-attacks, Dynamic Load Altering Attacks (D-LAAs) [7], [8] were designed to destabilise the network by controlling some compromised loads (e.g., electric vehicles, appliances, smart factories) in a coordinated way.

The present paper proposes a control scheme to defend against D-LAAs by using the flexibility offered by Energy Storage Systems (ESSs). The proposed control strategy is structured into two phases: (i) the off-line optimal placement of ESSs over the buses of the protected transmission network; (ii) the synthesis of an on-line control law that assures the stability of the network against the set of considered D-LAAs.

The remainder of the paper is organised as follows: Section 2 presents the needed preliminaries on network modeling and D-LAAs, together with the design of the on-line stabilizing control law; Section 3 discusses the optimal placement strategy of the ESSs over the network; Section 4 provides a validation scenario where a destabilizing D-LAA is demonstrated on a simple test network in both an uncontrolled and a controlled setting; Section 5 presents the result of the optimal ESS placement over a standard test network, the IEEE-14; Section 6 draws the conclusions and highlights future works.

II. RELATED WORKS

CPSs are a contact point between computer science and control theory. Due to the deep linkage between the cyber and the physical domains that characterize CPSs, properties such as stability and robustness are typically studied together with concepts such as data integrity and intrusion detection.

The concept of security is of the utmost importance in the CPSs literature, as several critical systems, such as utility networks, transport infrastructures and healthcare systems, have been modelled as CPSs. In general, a secure CPS provides guarantees on both the integrity of its data handling pipeline and on the safety of its physical process. In order to assure the safe operation of a CPS it is typically required to design a controller able to maintain certain critical quantities (e.g., temperature, voltage, pressure, ...) within some operative bounds, even when the CPS is subject to some form of adverse attack or event.

In this direction, CPSs have been widely modeled and studied as linear time-invariant descriptor systems [9]–[11], that represent the CPS dynamics with differential equations and algebraic constraints. By properly designing the inputs and disturbances of such systems, researchers were able to model a wide range of attacks that may affect a CPS [10], such as state attacks (e.g., actuator or physical attacks), output attacks (e.g., data injection attacks) and even integrity attacks, that compromise the control logic of a portion of a CPS.

The cyber-attacks we consider in this work are the so-called Dynamic Load Altering Attacks (D-LAAs) [8], a complex dynamical attack that follows a control logic to employ a set of compromised electrical loads (e.g., loads that were part of a demand-side management program) with the aim of steering the transmission network towards instability. Several works studied such attacks, from both the defendant [12]–[14] and attacker perspective [15], highlighting how the diffusion of demand-side management programs and large-scale controllable loads, such as smart factories and EV fleets, may introduce a significant vulnerability into the network.

This paper proposes a control scheme to defend against D-LAAs by using the flexibility offered by (ESSs). The proposed control strategy is structured into two phases: (i) the off-line optimal placement of ESSs over the buses of the protected transmission network; (ii) the synthesis of a on-line control law that assures the stability of the network against the set of considered D-LAAs.

III. Problem Fomulation

A. Preliminaries on Dynamic Load Altering Attacks

In this work, we will design a controller to defend against D-LAAs, which were originally introduced in [8]. This kind of attack is aimed at destabilising the transmission network by controlling some vulnerable loads in a closed loop fashion. This feedback can be obtained by the attacker by exploiting compromised network equipment. It was shown in [8] that a properly defined dynamic attack law is able to steer the network towards instability in a limited amount of time.

In the previous work [14], the authors proposed a state feedback controller to robustly stabilize transmission networks against D-LAAs by employing Energy Storage Systems (ESSs) to provide a regulating action on the network. To this end, it was shown that a transmission network vulnerable to a set of D-LAAs of the form $P_v^{LV}(t) = -K_{vs}^{LG}(t)\omega_s(t)$ can be modelled as the parametric linear time variant system:

$$\begin{bmatrix}\dot{\delta}\\ \dot{\theta}\\ \dot{\omega}\end{bmatrix} = A\begin{bmatrix}\delta\\ \theta\\ \omega\end{bmatrix} + Bu = \\ = (A_1 + A_2)\begin{bmatrix}\delta\\ \theta\\ \omega\end{bmatrix} - \begin{bmatrix}0\\ (-D^L)^{-1}\\ 0\end{bmatrix}\bar{u}_T, \tag{1}$$

with

$$A_1 = \begin{bmatrix}0 & 0 & I\\ (-D^L)^{-1}L_{lg} & (-D^L)^{-1}L_{ll} & 0\\ M^{-1}(L_{gg}+K^I) & M^{-1}L_{gl} & M^{-1}(D+K^P)\end{bmatrix} \tag{2}$$

and

$$A_2 = \begin{bmatrix}0 & 0 & 0\\ 0 & 0 & (-D^L)^{-1}K^{LG}(t)\\ 0 & 0 & 0\end{bmatrix}, \tag{3}$$

The network model is the result of a DC (Direct Current) linearization [16], a linearization technique based on the following assumptions:

- angular differences are small

$$|\delta_i(t) - \theta_j(t)| \ll 1 \ \forall L_{gl}(i,j) \neq 0$$
$$|\theta_i(t) - \theta_j(t)| \ll 1 \ \forall L_{ll}(i,j) \neq 0;$$

- the network is lossless;
- the bus voltage magnitudes are constant and equal to their nominal values.

The Laplacian matrix L of the graph representation of the network is represented by the matrix

$$L = \left[\begin{array}{c|c} \overbrace{L_{gg}}^{(n\times n)} & \overbrace{L_{gl}}^{(n\times m)} \\ \hline \underbrace{L_{lg}}_{(m\times n)} & \underbrace{L_{ll}}_{(m\times m)} \end{array}\right]$$

, composed by the following blocks:

- L_{gg} is *diagonal*;
- L_{gl} contains nonzero-elements in correspondence to a direct generator bus - load bus connection;
- L_{lg} is the transpose of L_{gl};
- L_{ll} represents the load bus connections.

The model (1) takes into account the sensitivities of the load to the frequency variations using the diagonal damping matrix D^L, similarly, the generators damping are modelled through diagonal matrix D. The inertia of the power system is represented by the diagonal matrix M in which each element is characterized by the inertia associated to the respective generator. In what follows, we assume that the speed control of each generator can be modeled as a PI control, thereafter, K^P and K^I entries represent, respectively, the integral and proportional controller coefficients of the generators at all generator buses [16]. Using a parametric uncertainties model approach, the transition matrix A can be split in two parts, the nominal dynamics of the network, indeed not subject to attacks, and the second part, which introduces the dynamics of the attacks and their impacts on the dynamics of the whole system. Respectively, the nominal and the attacked dynamics are represented by matrices A_1 and A_2. The term $\bar{u}_T$ represents the input of the system. Physically, the inputs are the power deviations (injections or withdraws) with respect to the operative point around which the system (1) is linearized on the various buses. For our

purpose, the input of the system, $\bar{u}_T$, can be split into two terms: $\bar{u}_T = P^L + u$, the term P^L represents the power consumption at load buses, that can be used by the attacker to induce a frequency deviation that then may feed a D-LLAs, and the component u representing the ESS controlled power that implements the state feedback control $u = K[\delta, \theta, \omega]^T$ to robustly stabilize the network.

Due to the structure of (1), the effects of D-LAAs can be seen as a form of parametric uncertainty affecting the nominal transition matrix of the network A. In [14], the system (1) was studied as a switched system with polytopic uncertainty, and utilising the results from [17] it was proven that it was possible to design a controller of the form $u(t) = Kx(t)$ able to defend against the set of considered D-LAAs, provided that the controller knows which buses are vulnerable and is provided with an estimation of the maximum power that can be compromised by the attackers. The authors proved that to determine the value of the control gain K it was sufficient to solve the multi-objective optimization problem (whose objectives are weighted by the parameters $\gamma_1, \gamma_2, \gamma_3$):

$$\begin{aligned} \max_{P,Y,\alpha,\bar{u}_{max}} \quad & \gamma_1 \; tr(P) - \gamma_2 \; \bar{u}_{max} \; + \; \gamma_3 \; \alpha \\ & \text{s. t.} \quad \forall i = 1, ..., p \\ & \begin{bmatrix} A_i P + P A_i^T + BY + Y^T B^T & P \\ P & -I/\alpha \end{bmatrix} < 0 \\ & \begin{bmatrix} P & Y^T \\ Y & \bar{u}_{max} I \end{bmatrix} \geq 0 \\ & P = P^T \end{aligned} \tag{4}$$

and set $K = YP^{-1}$.

A challenge faced in [14] is related to the fact that the matrix K is in principle dense, which has some technical implications related to the physical meaning of the product $Kx(t)$. In particular, to protect the network with the proposed strategy, one would need:

1) access to the state measurements on all of the network nodes, as the matrix K does not have any column of zeroes (i.e., the vector $x(t)$ is required in its entirety to compute $u = Kx(t)$);
2) the presence of an ESS on every network node, as the matrix K does not have any row of zeroes (i.e., the vector $u = Kx(t)$ does not have any structurally zero elements).

These two limitations significantly impact the likelihood of deploying the control strategy of [14], as the technological requirements imposed to the operator may be too demanding, for both economic and logistic constraints. In a realistic scenario, the number of installed ESSs will be limited to a few units, and their possible locations will include a limited subset of secured buses, $\mathcal{M}_p$, previously identified.

In [14], it was show that, due to the particular structure of the closed form $K = YP^{-1}$, it is always possible to avoid the placement of a storage on a specific node by setting a constraint in the optimisation problem (4), to force the elements of the corresponding row of the matrix Y to be zero. The open limitation affecting [14] was related to the placement of the ESSs, as their position in the network may have a significant impact on the defence performance. In fact, it was assumed that the network operator was free to deploy a storage on each of the buses in the set $\mathcal{M}_p$, but the identification of an optimal criteria for determining such set remained an open problem.

The algorithm presented in this paper aims at identifying the optimal placement strategy for ESSs over a minimal subset of $\mathcal{M}_p$, so that their number is minimized. To do so, the following subsection discusses a solution for the optimal placement of ESSs.

B. Optimal ESSs placement

To determine the optimal locations to install the ESSs, the transmission network is modelled as a weighted and connected graph, in which the weights are given by the impedences of the links between buses. Our goal is to find a prioritisation criteria to sort the secured buses in the set $\mathcal{M}_p$ that are candidates to host an ESS and, to this end, we designed an ad-hoc value function.

The nature of D-LAAs is to modify the power load on the nodes dynamically, based on measurements from a subset of state variables. This attack modifies the power flows through the network, in order to steer the generator frequencies outside of their operative regions (recall that, in our setting, for its structure the attack is based on the frequency deviation at the generator buses). To defend against such an attack, the optimal storage placement shall take into account two different concepts, as the ESSs have to:

1) reduce the power flow deviations from nominal values;
2) relieve the affected generators to support their synchronization.

The optimal configuration sought by the algorithm is then characterised by a certain number of ESSs distributed over the network, so that their distance from vulnerable buses (i.e. potential attacks) and generators are both minimised and balanced.

In fact, on the one hand, having ESSs displaced too far from the vulnerable buses would imply that the contribution of the ESSs would be filtered by the power network, requiring a considerable control effort when the attack is located far from the defence/ESS location. On the other hand, having ESSs located near the generators allows to unload the on-board regulating systems of the generators, partially uncoupling the disturbances generated on the network from the self-regulating control actions.

Having set this criterion, we now need to define in our setting the concept of distance between two nodes. A natural quantity that serves the purpose of "electrical distance" when dealing with power networks is the minimum impedance observed on the paths that connect two nodes. To compute this quantity it is sufficient to employ off-line an implementation of the Dijkstra algorithm, whose complexity in the considered setting is treatable, as it is linear in the number of buses and linearithmic in the number of lines [18].

Having these concepts in mind, the value function has to capture the cumulative electrical distance (impedance) a given location has with respect to the set of vulnerable nodes and the generators. This can be obtained by setting, for every node $i \in |\mathcal{M}_p|$, a value index d_i:

$$\begin{aligned} d_i =& \rho_a \sum_{j|x_j \in M_a} \phi(Z,i,j) + \rho_g \sum_{j|x_j \in M_g} \phi(Z,i,j) \ \forall i \in |\mathcal{M}_p| \\ & \rho_g = 1 - \rho_a, \quad \rho_a \in [0,1] \end{aligned} \tag{5}$$

where $\mathcal{M}_a$ and $\mathcal{M}_g$ are the set of vulnerable and generator nodes respectively, $\phi(Z,i,j)$ is the minimum impedance between the nodes i, j, Z is the line impedance matrix and ρ_a and ρ_g are complementary coefficients that weight the operator's choice for the prioritization of the distance from vulnerable nodes and generators.

Having defined a value index d_i for every secured node in the network, it is now possible to sort and prioritise their locations for the optimal placement strategy. In the following, we will assume the nodes in $\mathcal{M}_p$ to be sorted in ascending order according to their values of d_i.

C. Optimisation algorithm

In the presentation above we neglected the aspects related to determining the minimum number of ESSs to be installed. The minimisation of ESSs is a crucial requirement for the operator, as their cost is not negligible. In order to find such minimum number, we propose an iterative procedure: starting from the empty set and adding to it, one by one, the remaining buses ordered according to their priority index d_i, find the minimum number of nodes for which (4) admits a solution.

In other words, iteratively increase $\mathcal{I}$ from 1 to $|\mathcal{M}_p|$, until

$$\begin{aligned} \max_{P,Y,\alpha,\bar{u}_{max}} \quad & \gamma_1 \ tr(P) - \gamma_2 \ \bar{u}_{max} \ + \ \gamma_3 \ \alpha \\ & \text{s. t.} \quad \forall i = 1,...,p \\ & \begin{bmatrix} A_i P + P A_i^T + B X Y + X Y^T B^T & P \\ P & -I/\alpha \end{bmatrix} < 0 \\ & \begin{bmatrix} P & Y^T X^T \\ XY & \bar{u}_{max} I \end{bmatrix} \geq 0 \\ & P = P^T \\ & X \text{ is diagonal} \\ & X(i,i) = x_i \ \forall i \in \mathcal{M}_p \text{ and } X(i,i) = 0 \text{ otherwise} \end{aligned} \tag{6}$$

becomes feasible.

The diagonal matrix X defines the structure of the controller: if the element (i,i) of the matrix X is zero, then the corresponding i^{th} row of the control as $U = Kx = XYP^{-1}x$ is zero, implying that no storage will be placed on node i, in line with [14].

The resulting algorithm is reported in Table **??**.

Once the placement is completed and the matrix K is determined, the control law can be deployed to defend against D-LAAs in real time.

Algorithm 1:

Result: Storage placement and controller
Sort the nodes $i \in \mathcal{M}_p$ according to the value function (5)
Initialize: $\mathcal{I}$ = 1; $x_i = 0 \ \forall$ nodes $i \in |\mathcal{M}_p|$
while $\mathcal{I} \leq |\mathcal{M}_p|$ **do**
  $x_i = 1 \ \forall i \leq \mathcal{I}$
  if (4) *has a solution* **then**
    $K = YP^{-1}$
    Output: Set of nodes for ESSs placement, given by $\mathcal{I}$;
    Defence control law, defined by its gain K
  else
    $\mathcal{I} \leftarrow \mathcal{I} + 1$
  end
end
Output: No placement protects from the given attacks

It can be remarked that in principle (6) could be solved to also directly minimize $\mathcal{I}$. This direct minimization would in turn require the solver to deal with binary decision variables in a LMI setting, significantly increasing the problem complexity, which makes the proposed sorting-based solution more appealing for real-world applications.

IV. Real-Time Controller and D-LAA Validation Scenario

In this section we consider the *IEEE 9 bus test system* reported in Figure 1 to validate the proposed real-time defence control law and the capabilities of the D-LAAs. In particular, Section IV-A describes the scenario considered and details the attack sequence implemented, also demonstrating how the attack is able to de-stabilize the network in the uncontrolled case, while Section IV-B reports the effects of the proposed real-time control law for the protection of the network.

A. Reference Scenario

From an attack point of view, we consider a scenario in which two different attacks are deployed: one on the node 5, driven by the frequency deviation of generator 1, and one on the bus 9, driven by the the frequency deviation of the generator 2. For our initial testing, we modified the standard network by adding the presence of one ESS on the node 7. The attack gains $-K_{vs}^{LG}$ are bounded respectively by the values of 20 and 10. In all the simulations we will consider attacks based on a measurements from all generator buses. The modeled sequence of attacks consists of the following:

1) an initial static load altering attack on nodes 5 and 9 of 0.1 $p.u.$, from time $t = 1s$ to $t = 2s$, to induce a non-negligible frequency deviation in the network;
2) a D-LAA on node 5 from time $t = 3s$ to $t = 12s$, with maximum attack gain;

3) a D-LAA on node 9 from time $t = 7s$ to $t = 22s$, with maximum attack gain;
4) a static load altering attack on nodes 5 and 9 of $0.01\ p.u.$, from time $t = 21s$ to $t = 22s$, to further perturb the network;
5) two contemporary D-LAAs on nodes 5 and 9, respectively, from times $t = 21s$ and $t = 23s$, up to times $t = 36s$ and $t = 40s$, with their corresponding maximum attack gains.

Figure 2 reports the attack sequence: the first plot shows the time evolution of the static load altering attacks on nodes 5 and 9, while the second one represents the percentage of the attack gain for the D-LAA on node 5 and the last graph represents the same quantity for node 9.

Figure 3 shows how, for the uncontrolled case (i.e., when the ESS is deactivated), the D-LAA, exploiting the frequency deviation generated by the initial Static Load Altering Attack (S-LAA) is able to induce an unstable behaviour in the network.

Figure 4 reports the magnitude of the attacks expressed in p.u., highlighting how power is injected in the network when the generator is in sub synchronous and vice versa. This counter-phase power injection, guided by a state feedback attack, is due to the unstable eigenvalues induced in the system by the D-LAAs [8] and is able to destabilise the system in a few seconds. This can be esily seen from the comparison of the Figures 3 and 4, where it is possible to see that all the generators go out of the operational range ($|\omega_i| < 2$) [8] around $t = 9s$. We mention that the linearized model becomes inaccurate when the generators' frequencies are steered away from their nominal equilibrium values.

In what follows, we will consider a scenario in which an anomaly detection system (IADS) [19]–[21] is utilised to detect ongoing attacks from the analysis of data coming from the Supervisory Control and Data Acquisition (SCADA) system to provide better situational awareness to the defence controllers. In this perspective, the ESSs are not utilised to regulate the network if an attack is not detected, as it is a reasonable assumption that ESSs are employed to only defend against ongoing attacks ands compensate significant frequency deviations. For this reason, the ESS are not to be considered as a virtual inertia to cover the normal network imbalance, but should be fed and maintained at some specific value of charge [21], [22], in order to be ready to interview in case of need.

Under the assumptions of the presence of IADS and the independence of the control action w.r.t. the State of Charge (SOC) of the ESS, we are then able to demonstrate the effectiveness of the proposed state feedback controller.

B. Controlled scenario

Activating the control action for the ESS on node 7, we demonstrate in this section that the network is successfully stabilised and the attack is compensated.

Figure 5 shows the frequency deviations on the generators, while Figure 6 shows the shape and the magnitude of the attacks. The presence of the pre-emptive S-LAA from $t = 1$ to $t = 2$ is designed in order to induce a initial unbalance in the network, so that the following Dynamic Load Altering Attack (D-LAA)s will meet favourable conditions to be effective [8].

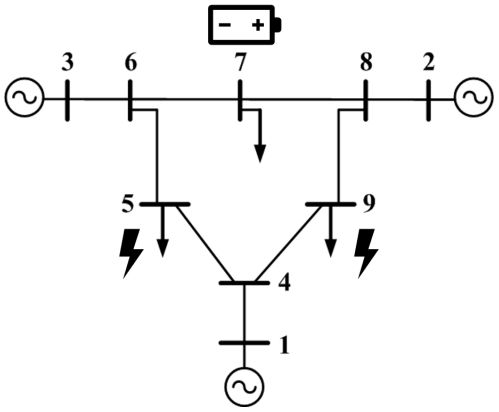

Fig. 1: Modified IEEE 9 bus test system

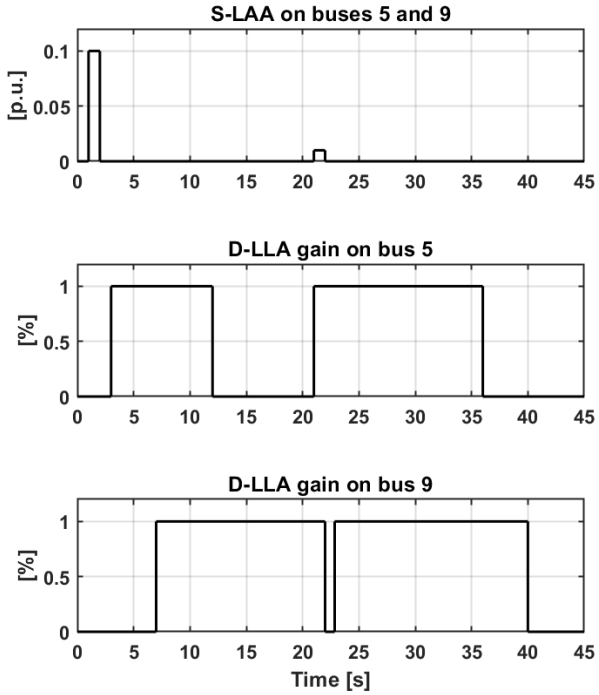

Fig. 2: Attacks sequence on IEEE 9 bus test system

For the sake of presentation, we assume that the first S-LAA is not recognized as an attack by the IADS, implying that the ESS control is not activated. Exploiting the unbalance generated by the S-LAA an D-LAA starts on the node 5, driven by the frequency deviation arisen on generator 1 at time $t = 3s$. This attack (reported in the first plot of Figure 6) start to excite the unstable modes of the system (see the zoom in Figure 5), as at this stage the defense strategy is not yet activated. At $t = 7$, a second D-LAA arises on node 9,

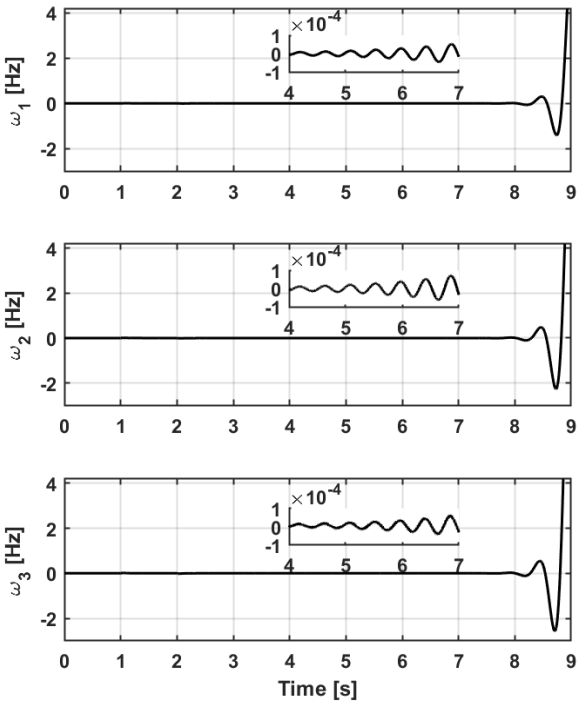

Fig. 3: Frequency deviation of the uncontrolled IEEE 9 bus test system case

driven by the the frequency deviation measured on generator 2. In this scenario, we assume that the IADS recognises the ongoing attacks a time 7.5, activating hence the control. The effect of the control are related to the minimization of the frequency deviations that drive the attacks, meaning that, due to the state feedback nature of the D-LAAs, by regulating the network frequencies the ESSs are able also to annihilate the attacking power. We recall that the identified controller, obtained solving the optimization problem (4), asymptotically stabilizes the network robustly with respect to all the possible combinations of the considered D-LAAs. The rejection effect that the controller attains against the D-LAAs is shown in Figure 6.

Figure 7 reports the power injection on the controlled node 7: when at the time 7.5 the IADS recognizes the abnormal behavior, the controller is triggered. The measured frequency deviation generates a spike in the control effort, but after this peak has some regulating effects on the on-going attack, the control magnitude reduces significantly.

For the sake of comparison, Figure 8 reports the control action if the IADS is able to recognize the anomaly in a more efficient way, activating the control at time $t = 6s$.

An important difference between D-LAA and S-LAA resides in the fact that S-LAA are not able to move the eigenvalue of the network to the instability region [8], but they are still necessary to introduce a frequency deviation needed to activate the D-LAA. In the considered scenario, a second S-LAA is then applied from time $t = 21s$ to $t = 22s$

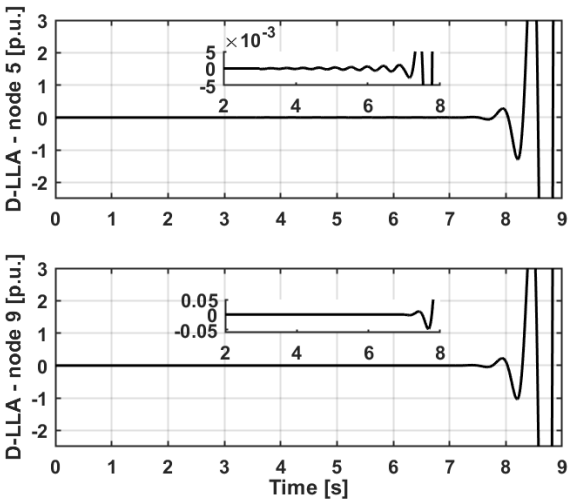

Fig. 4: D-LAA magnitude of the uncontrolled IEEE 9 bus test system case. First plot shows the attack node 5, related to the frequency deviation ω_1 of generator 1, second plot shows the attack on node 9 driven by the frequency deviation ω_2 on generator 2

on nodes 5 and 9, with the purpose to create an addition frequency deviation to amplify the D-LAAs. Note that the defence strategy obtained from the optimization problem (4) is not designed to face S-LAAs, but the asymptotic stability property of the controlled system brings the induced frequency deviation to zero (see zoom in Figure 5 between time 20 and 25). The drawback of employing ESSs to respond to such attacks consists in the request of a non-negligible control effort from the ESS, as depicted by the spikes of Figure 7.

V. Simulations with optimal ESS placement

In this section we will demonstrate on the test network IEEE-14 the optimal ESS placement procedure to defend against the considered D-LAAs. With reference to Figures 9, we now consider three different classes of attacks:

1) YELLOW attacks: attacks that are spread all over the network
2) RED attacks: attacks that are concentrated in a single mesh of the network
3) PURPLE attacks: attacks that are concentrated on generation nodes.

The two Figures detail the attack locations on their corresponding test networks.

A. Unsecured IEEE-14 bus test system

In our first testing the 14 bus test system IEEE will be used to test the placement algorithm. We bound the gains of all the attacks reported in 9 with a maximum value of 10^6. In particular, the attacks considered are color-coded as follows:

- YELLOW attacks, that are spread over the network, on nodes $2, 7, 11, 13$

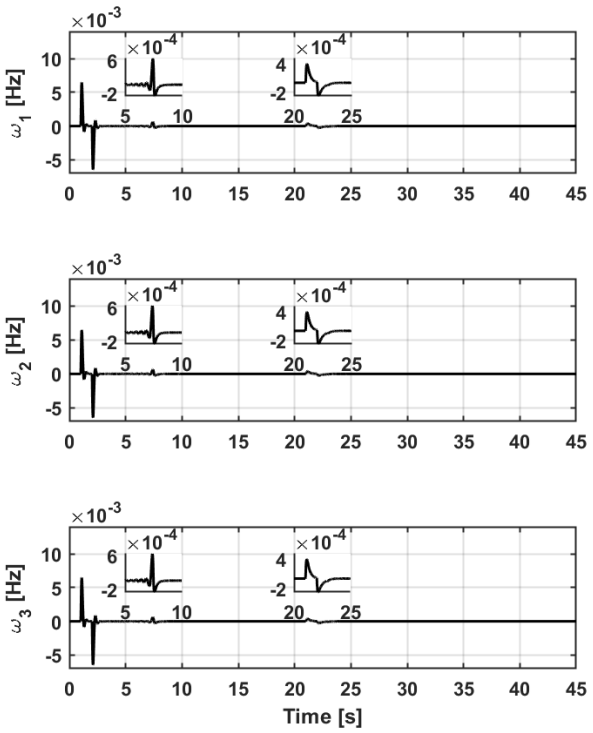

Fig. 5: Frequency deviation of the controlled IEEE 9 bus test system case

TABLE I: ESSs placement-14 bus-Yellow and PURPLE Attacks

Weights		Yellow Attacks	Purple Attacks
ρ_a	ρ_g	$\mathcal{M}_p^*$	$\mathcal{M}_p^*$
1.0	0.0	{9,14}	{2,5,4}
0.7	0.3	{5,9}	{2,5,4}
0.5	0.5	{5,4}	{2,5,4}
0.3	0.7	{5,4}	{2,5,4}

- RED attacks, that are located in a single mesh, on nodes $10, 11, 13, 14$
- PURPLE attacks, that are on the generator buses, on nodes $1, 3, 6, 8$.

Tables I and II report the results of the optimal placement problem. In particular, in Table I YELLOW and PURPLE attacks are considered for various values of ρ_a and ρ_g. Overall, all proposed placements are similar, with minor changes in the prioritization of the buses due to the different definitions of d_i. The contribution of the weights ρ_a and ρ_g becomes more significant in the case of protection against RED attacks, as reported in Table II. From the table, we can note how when the position of the generators is not considered (i.e., $\rho_g = 0$) the number of the ESSs required for the robust stabilization is 3, as the aggregation of the attacks drives the placement in a limited area with the intent

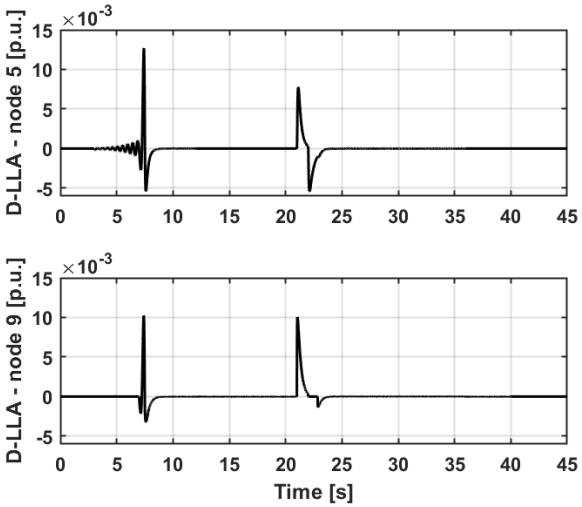

Fig. 6: D-LAA magnitude of the controlled IEEE 9 bus test system case. First plot shows the attack node 5, related to the frequency deviation ω_1 of generator 1, second plot shows the attack on node 9 driven by the frequency deviation ω_3 on generator 3

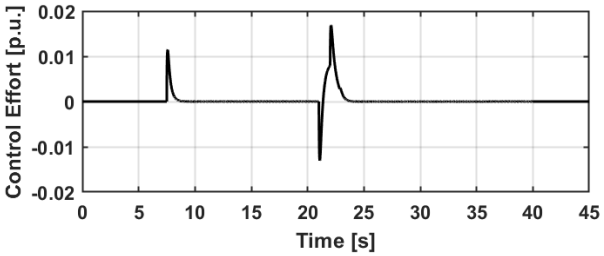

Fig. 7: Control action on node 7

of absorb/redirect the flows of power caused by the attack as soon as they start affecting the network. Balancing the weights (e.g., the case $\rho_a = \rho_g = 0.5$) the algorithm is able to find a solution that involves the presence of only 2 ESSs, placed on buses that divide the zone under attack (top) from the secure (bottom) one. Setting the weights as $\rho_a = 0.3$ $\rho_g = 0.7$ moves the *center-of-mass*, with respect to the electrical distance defined in (5), of the network in the lower portion of the network. As a consequence, the network is divided by the nodes 5 and 4 instead of 6 and 9, with the need of an additional protection on node 2 to better defend the generators.

VI. Conclusions and Future Works

This paper presented an optimization algorithm to determine the optimal placement for Energy Storage Systems (ESSs) to protect a transmission network vulnerable to Dynamic Load Altering Attacks. The designed algorithm exploits the geometrical structure of the attack to synthesize a defence control law for ESSs able to robustly stabilize the network against any combination of the considered attacks.

The optimal placement obtained was demonstrated to be able to protect the network against various types of attacks on

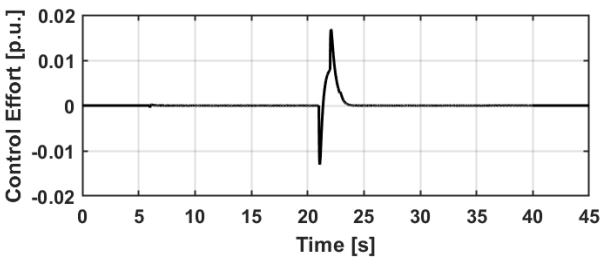

Fig. 8: Control action on node 7 - efficient IADS

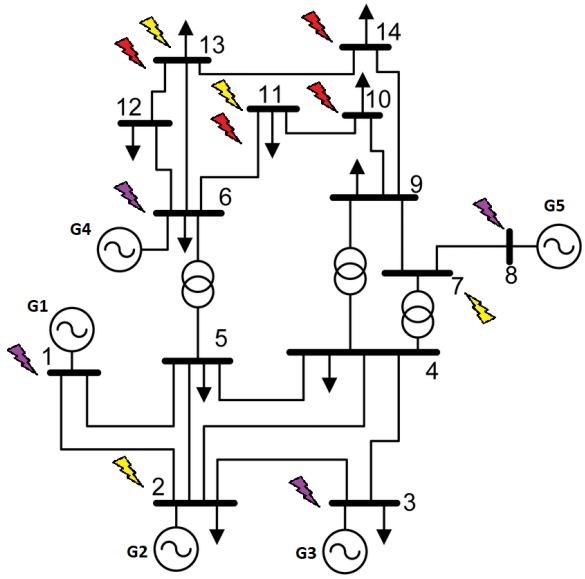

Fig. 9: Unsecured IEEE-14 bus test system- In red, YELLOW and PURPLE the considered attacks.

the IEEE-14 test network. Future research directions involve the explicit inclusion of the ESS capacity and its state-of-charge-dynamics in the placement problem.

TABLE II: ESSs placement-14 bus-Red Attack

Weights		Red Attacks
ρ_a	ρ_g	$\mathcal{M}_p^*$
1.0	0.0	{6,12,9}
0.7	0.3	{6,12,9}
0.5	0.5	{6,9}
0.3	0.7	{2,5,4}

REFERENCES

[1] D. Groppi, A. Pfeifer, D. A. Garcia, G. Krajačić, and N. Duić, "A review on energy storage and demand side management solutions in smart energy islands," *Renewable and Sustainable Energy Reviews*, vol. 135, p. 110183, Jan. 2021.

[2] R. Jing, M. N. Xie, F. X. Wang, and L. X. Chen, "Fair p2p energy trading between residential and commercial multi-energy systems enabling integrated demand-side management," *Applied Energy*, vol. 262, p. 114551, Mar. 2020.

[3] E. L. Karfopoulos and N. D. Hatziargyriou, "Distributed coordination of electric vehicles providing v2g services," *IEEE Transactions on Power Systems*, vol. 31, no. 1, pp. 329–338, Jan. 2016.

[4] C. Kwon and I. Hwang, "Cyber attack mitigation for cyber–physical systems: hybrid system approach to controller design," *IET Control Theory & Applications*, vol. 10, no. 7, pp. 731–741, Apr. 2016.

[5] F. Pasqualetti, F. Dorfler, and F. Bullo, "Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design," in *IEEE Conference on Decision and Control and European Control Conference*. IEEE, Dec. 2011.

[6] K. Chatterjee, V. Padmini, and S. A. Khaparde, "Review of cyber attacks on power system operations," in *2017 IEEE Region 10 Symposium (TENSYMP)*. IEEE, Jul. 2017.

[7] S. Amini, H. Mohsenian-Rad, and F. Pasqualetti, "Dynamic load altering attacks in smart grid," in *2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, Feb. 2015.

[8] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: Attack models and protection schemes," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2862–2872, July 2018.

[9] "Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems," *IEEE Control Systems*, vol. 35, no. 1, pp. 110–127, Feb. 2015. [Online]. Available: https://doi.org/10.1109/mcs.2014.2364725

[10] F. Pasqualetti, F. Dorfler, and F. Bullo, "Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design," in *IEEE Conference on Decision and Control and European Control Conference*. IEEE, Dec. 2011. [Online]. Available: https://doi.org/10.1109/cdc.2011.6160641

[11] ——, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013. [Online]. Available: https://doi.org/10.1109/tac.2013.2266831

[12] E. Baron-Prada, E. Osorio, and E. Mojica-Nava, "Resilient transactive control in microgrids under dynamic load altering attacks," in *2017 IEEE 3rd Colombian Conference on Automatic Control (CCAC)*. IEEE, Oct. 2017. [Online]. Available: https://doi.org/10.1109/ccac.2017.8276400

[13] A. Gusrialdi and Z. Qu, "Smart grid security: Attacks and defenses," in *Smart Grid Control*. Springer International Publishing, Sep. 2018, pp. 199–223.

[14] R. Germanà, A. Giuseppi, and A. Di Giorgio, "Ensuring the stability of power systems against dynamic load altering attacks: A robust control scheme using energy storage systems," in *2020 European Control Conference (ECC)*. IEEE, 2020, pp. 1330–1335.

[15] V. Katewa and F. Pasqualetti, "Optimal dynamic load-altering attacks against power systems," in *2021 American Control Conference (ACC)*. IEEE, May 2021.

[16] F. Pasqualetti, A. Bicchi, and F. Bullo, "A graph-theoretical characterization of power network vulnerabilities," in *Proceedings of the 2011 American Control Conference*, June 2011, pp. 3918–3923.

[17] B. Polyak and P. Shcherbakov, "Ellipsoidal approximations to attraction domains of linear systems with bounded control," in *2009 American Control Conference*. IEEE, 2009. [Online]. Available: https://doi.org/10.1109/acc.2009.5160175

[18] M. Barbehenn, "A note on the complexity of dijkstra's algorithm for graphs with weighted vertices," *IEEE Transactions on Computers*, vol. 47, no. 2, p. 263, 1998. [Online]. Available: https://doi.org/10.1109/12.663776

[19] V. Graveto, L. Rosa, T. Cruz, and P. Simões, "A stealth monitoring mechanism for cyber-physical systems," *International Journal of Critical Infrastructure Protection*, vol. 24, pp. 126 – 143, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1874548218300672

[20] F. Adamsky, M. Aubigny, F. Battisti, M. Carli, F. Cimorelli, T. Cruz, A. D. Giorgio, C. Foglietta, A. Galli, A. Giuseppi, F. Liberati, A. Neri, S. Panzieri, F. Pascucci, J. Proenca, P. Pucci, L. Rosa, and R. Soua, "Integrated protection of industrial control systems from cyber-attacks: the atena approach," *International Journal of Critical Infrastructure Protection*, vol. 21, pp. 72 – 82, 2018.

[21] A. Giuseppi, R. Germana, and A. Di Giorgio, "Risk adverse virtual power plant control in unsecure power systems," in *2018 26th Mediterranean Conference on Control and Automation (MED)*, 2018, pp. 1–9.

[22] A. Di Giorgio, F. Liberati, A. Lanna, A. Pietrabissa, and F. D. Priscoli, "Model predictive control of energy storage systems for power tracking and shaving in distribution grids," *IEEE Transactions on Sustainable Energy*, vol. 8, no. 2, pp. 496–504, 2017.